

ON THE MINIMUM DISTANCE OF ELLIPTIC CURVE CODES

JIYOU LI, DAQING WAN, AND JUN ZHANG

ABSTRACT. Computing the minimum distance of a linear code is one of the fundamental problems in algorithmic coding theory. Vardy [14] showed that it is an **NP**-hard problem for general linear codes. In practice, one often uses codes with additional mathematical structure, such as AG codes. For AG codes of genus 0 (generalized Reed-Solomon codes), the minimum distance has a simple explicit formula. An interesting result of Cheng [3] says that the minimum distance problem is already **NP**-hard (under **RP**-reduction) for general elliptic curve codes (ECAG codes, or AG codes of genus 1). In this paper, we show that the minimum distance of ECAG codes also has a simple explicit formula if the evaluation set is suitably large (at least $2/3$ of the group order). Our method is purely combinatorial and based on a new sieving technique from the first two authors [8]. This method also proves a significantly stronger version of the MDS (maximum distance separable) conjecture for ECAG codes.

1. INTRODUCTION

Let \mathbb{F}_q^n be the n -dimensional vector space over the finite field \mathbb{F}_q with q elements. For any vector $x = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$, the *Hamming weight* $\text{Wt}(x)$ of x is defined to be the number of non-zero coordinates, i.e.,

$$\text{Wt}(x) = \#\{i \mid 1 \leq i \leq n, x_i \neq 0\} .$$

A linear $[n, k]$ code C is a k -dimensional linear subspace of \mathbb{F}_q^n . The *minimum distance* $d(C)$ of C is the minimum Hamming weight of all non-zero vectors in C , i.e.,

$$d(C) = \min\{\text{Wt}(c) \mid c \in C \setminus \{0\}\} .$$

A linear $[n, k]$ code $C \subseteq \mathbb{F}_q^n$ is called a $[n, k, d]$ linear code if C has minimum distance d . A well-known trade-off between the parameters of a linear $[n, k, d]$ code is the Singleton bound which states that

$$d \leq n - k + 1 .$$

An $[n, k, d]$ code is called a *maximum distance separable* (MDS) code if $d = n - k + 1$. The *dual code* C^\perp of C is defined as the set

$$\{x \in \mathbb{F}_q^n \mid x \cdot c = 0 \text{ for all } c \in C\} ,$$

where $x \cdot c$ is the inner product of vectors x and c , i.e.,

$$x \cdot c = x_1 c_1 + x_2 c_2 + \dots + x_n c_n .$$

The work of Jiyou Li is supported by the National Science Foundation of China (11001170) and Ky and Yu-Fen Fan Fund Travel Grant from the AMS. The research of Daqing Wan is partially supported by NSF. This research of Jun Zhang is supported by the National Key Basic Research Program of China (2013CB834204), the National Natural Science Foundation of China (61171082, 10990011 and 60872025).

Computing the minimum distance of a linear code is one of the most important problems in algorithmic coding theory. It was proved to be **NP**-hard for general linear codes in [14]. The gap version of the problem was also shown to be **NP**-hard in [6]. And the same paper showed that approximating the minimum distance of a linear code cannot be achieved in randomized polynomial time to the factor $2^{\log^{1-\epsilon} n}$ unless $\text{NP} \subseteq \text{RTIME}(2^{\text{polylog}(n)})$. In [4], Cheng and the second author derandomized the reduction and showed there is no deterministic polynomial time algorithm to approximate the minimum distance to any constant factor unless $\text{NP} = \text{P}$. And they proved that approximating the minimum distance of a linear code cannot be achieved in deterministic polynomial time to the factor $2^{\log^{1-\epsilon} n}$ unless $\text{NP} \subseteq \text{RTIME}(2^{\text{polylog}(n)})$.

Despite the above complexity results, it is more interesting to compute the minimum distance of linear codes that are used in practical applications. An important class of such codes is algebraic geometry (AG) codes with parameters $[n, k, d]$ as defined in Section 4. The minimum distance of such AG codes from algebraic curves of genus g is known to satisfy the inequality

$$n - k - g + 1 \leq d \leq n - k + 1.$$

In the simplest case $g = 0$, i.e., generalized Reed-Solomon codes, the minimum distance has the simple formula $d = n - k + 1$. In the next simplest case $g = 1$, either $d = n - k$ or $d = n - k + 1$, and Cheng [3] showed that determining the minimum distance of ECAG codes between the two options is **NP**-hard under **RP**-reduction. For genus $g \geq 2$, there is no such complexity result so far. But it is believed to be an **NP**-hard problem as well.

We are interested in positive results for determining the minimum distance of ECAG codes. It was shown in [3], and also in [16] from a different aspect, that computing the minimum distance of an ECAG code is equivalent to a subset sum problem (SSP) in the group of rational points on the elliptic curve. We now make this more precise.

Let E be an elliptic curve over the finite field \mathbb{F}_q . Let G be the group of \mathbb{F}_q -rational points on the elliptic curve E . The Hasse bound shows that $||G| - (q+1)| \leq 2\sqrt{q}$. Let $D \subseteq G$ be a nonempty subset of cardinality n , which will be our evaluation set for ECAG code. For a positive integer $1 \leq k \leq n < |G|$ and element $b \in G$, let $N(k, b, D)$ be the number of k -subsets $T \subseteq D$ such that $\sum_{x \in T} x = b$. The counting version of the k -subset sum problem for the pair (G, D) is to compute $N(k, b, D)$. The minimum distance of the ECAG $[n, k]$ -code is equal to $n - k$ if and only if the number $N(k, b, D)$ is positive. This k -subset sum problem is in general **NP**-hard if the evaluation set D is small. On the other hand, the dynamic programming method implies that there is a polynomial time algorithm to compute $N(k, b, D)$ if $n = |D|$ is large, say, $n = |G|^\delta$ for some constant $\delta > 0$.

In this paper, we obtain an asymptotic formula for $N(k, b, D)$ if $n = |D|$ is suitably large, say, $|D| > (\frac{2}{3} + \epsilon)|G|$. As an application, we show that if the cardinality n of the evaluation set is suitably large (at least $2/3$ of the group order), then the minimum distance of an ECAG code $[n, k]$ is always $n - k$. We conjecture that the condition $|D| > (\frac{2}{3} + \epsilon)|G|$ in our results can be improved to $|D| > (\frac{1}{2} + \epsilon)|G|$. Our main technical tool is the sieve method of the first two authors [9].

To describe the asymptotic formula, we introduce more notations. Let \widehat{G} be the group of additive characters of G . Note that \widehat{G} is isomorphic to G . Define

$$\Phi(D) = \max_{\chi \in \widehat{G}, \chi \neq \chi_0} \left| \sum_{a \in D} \chi(a) \right|.$$

Our main technical result is the following asymptotic formula for $N(k, b, D)$.

Theorem 1.1. *Notations as above. We have*

$$\begin{aligned} \left| N(k, b, D) - |G|^{-1} \binom{n}{k} \right| &\leq \frac{|S|}{|G|} \binom{\Phi(D) + k - 1}{k} + \frac{1}{|G|} \binom{\frac{n + \Phi(D)}{2}}{k} \\ &\quad + \frac{1}{|G|} \sum_{\substack{2 < d \leq k \\ d | \exp(G)}} \phi(d) \binom{\frac{n + \Phi(D)}{d} + k - 1}{k}, \end{aligned}$$

where S is the set of characters in \widehat{G} which have order greater than k and $\exp(G)$ is the exponent of G .

We apply this theorem to determine the minimum distance of ECAG codes (for details see Section 4) and obtain

Theorem 1.2. *Suppose that $n \geq (\frac{2}{3} + \epsilon)q$ and $q > \frac{4}{\epsilon^2}$, where ϵ is positive. There is a positive constant C_ϵ such that if $C_\epsilon \ln q < k < n - C_\epsilon \ln q$, then ECAG codes $[n, k]$ have the deterministic minimum distance $n - k$.*

If we allow the length of the codes to be larger, we then have a better bound on k .

Theorem 1.3. *If $n \geq q + 2$, then for $q > 64$ and $3 < k < q - 1$, then ECAG $[n, k]$ codes have the deterministic minimum distance $n - k$.*

Since one can check the cases $q \leq 64$ by a computer search, we have a complete result for the minimum distance of the ECAG code $[n, k]$ if $n \geq q + 2$. This gives a new proof of MDS conjecture on ECAG codes, in a purely combinatoric method. We now explain this application and its improvement.

Recall that an $[n, k, d]$ code is called a *maximum distance separable* (MDS) code if $d = n - k + 1$. MDS codes have a lot of advantages [10]. However, MDS codes are very rare, and so far, not too many MDS codes have been found. The Main Conjecture on MDS Codes states that for every linear $[n, k]$ MDS code over \mathbb{F}_q , if $1 < k < q$, then $n \leq q + 1$, except when q is even and $k = 3$ or $k = q - 1$, in which cases $n \leq q + 2$.

The most well-known MDS codes are Reed-Solomon codes. Since the evaluation set of a Reed-Solomon code can not exceed the finite field, the MDS conjecture always holds in this case. The MDS conjecture was proved whenever $q \leq 11$ or $k \leq 5$ by using the theory of finite geometries. Since the most popular candidates for MDS codes are the Goppa codes constructed from algebraic curves of small genus and algebraic geometry (AG) codes, people turned to concentrate the MDS conjecture for AG codes. As AG codes have algebraic and geometric properties, there are a lot of new algebraic-geometric methods to apply, while the general MDS property is more of a combinatorial property. The MDS conjecture for ECAG codes was first proved by Katsman and Tsfasman in [7]. Munuera [11] translated the conjecture for AG codes to another conjecture concerning the arithmetic of the curves. He then proved it for codes arising from elliptic curves, and curves of genus

2 when $q > 83$. Walker [15] presented a new approach to the problem in the case of elliptic curves by proving a statement about the geometry of the curve after a certain embedding.

In the case of hyperelliptic curves, for fixed genus g , Moer [5] showed that MDS conjecture holds when q is big enough. Chen [1] proved that there is a constant $C(g)$ depending only on the genus g such that the MDS conjecture is true when $q > C(g)$. And later in [2] Chen and Yau gave an upper bound of $C(g)$ which not only affirmatively answered the question asked by Munuera in [11], but also improved the result in [5] a lot.

As we pointed out that the minimum distance of an ECAG code has only two options and determining it is equivalent to an SSP problem, the MDS conjecture on ECAG codes is naturally reduced to a subset sum problem of the group of rational points on the elliptic curve. By Theorem 1.3, we have

Theorem 1.4. *For $q > 64$, MDS conjecture for ECAG codes holds.*

By Theorem 1.2, if some restriction on the dimension k is allowed, we can significantly improve the lower bound $q + 2$.

Theorem 1.5. *Suppose that $n \geq (\frac{2}{3} + \epsilon)q$ and $q > \frac{4}{\epsilon^2}$, where ϵ is positive. Then there is a positive constant C_ϵ such that if $C_\epsilon \ln q < k < n - C_\epsilon \ln q$, then there is no MDS ECAG code with parameter $[n, k]$.*

For small k , one can directly check if the ECAG code is MDS or not. For large k , by the duality, it can be reduced to the former case. From Theorem 1.5, we shall see that to get a long MDS code for fixed alphabet size q , Reed-Solomon codes are always the best choices.

This paper is organized as follows. Section 2 recalls the sieve method of the first two authors. Section 3 uses the sieve method to get an estimate of counting subset sum problems on any large subset of the rational point group of an elliptic curve. And Section 4 describes the relation between minimum distance of ECAG codes and subset sum problems on the evaluation set of the ECAG code. The main theorems of this paper then follow.

2. A DISTINCT COORDINATE SIEVING FORMULA

In this section we introduce a sieving formula discovered by Li-Wan [8]. It significantly improves the classical inclusion-exclusion sieve in several important cases. We recite it here without proof. For details and related applications, we refer to [8, 9]. Before we present the sieving formula, we introduce some notations valid for the whole paper.

- Let D be an alphabet set, X a finite set of vectors of length k over D .
- Denote $\overline{X} = \{(x_1, x_2, \dots, x_k) \in X \mid x_i \neq x_j, \forall i \neq j\}$ the pairwise distinct component subset.
- Let S_k be the symmetric group on $\{1, 2, \dots, k\}$. For $\tau \in S_k$, the sign function is defined to be $\text{sign}(\tau) = (-1)^{k-l(\tau)}$, where $l(\tau)$ is the number of cycles of τ including the trivial cycles which have length 1.
- Let $\tau = (i_1 i_2 \dots i_{a_1})(j_1 j_2 \dots j_{a_2}) \dots (l_1 l_2 \dots l_{a_s})$ with $1 \leq a_i, 1 \leq i \leq s$ be any permutation, denote the τ -symmetric subset

$$X_\tau = \left\{ (x_1, \dots, x_k) \in X \mid x_{i_1} = \dots = x_{i_{a_1}}, \dots, x_{l_1} = \dots = x_{l_{a_s}} \right\}. \quad (2.1)$$

- Let $f(x_1, x_2, \dots, x_k)$ be a complex valued function defined on X . Denote the distinct sum

$$F = \sum_{x \in \overline{X}} f(x_1, x_2, \dots, x_k),$$

and the τ -symmetric sum

$$F_\tau = \sum_{x \in X_\tau} f(x_1, x_2, \dots, x_k).$$

We now present the sieving formula found in [8].

Theorem 2.1. *Let F and F_τ be defined as above. Then*

$$F = \sum_{\tau \in S_k} \text{sign}(\tau) F_\tau. \quad (2.2)$$

We notice that in this formula, there are at most $k!$ terms (computable in many cases), which is significantly smaller than $2^{\binom{k}{2}}$, the needed number of terms by traditional sieving approach.

For $\tau \in S_k$, let $\overline{\tau}$ denote the conjugacy class determined by τ whose elements are permutations conjugate to τ . Conversely, in the case that we denote a conjugacy class by $\overline{\tau} \in C_k$, τ is a correspondent representative permutation. Since two permutations in S_k are conjugate if and only if they have the same type of cycle structure, C_k is exactly the set of all partitions of k .

The symmetric group of k elements, S_k , acts on D^k naturally by permuting coordinates. Given $\tau \in S_k$ and $x = (x_1, x_2, \dots, x_k) \in D^k$, $\tau \circ x = (x_{\tau(1)}, x_{\tau(2)}, \dots, x_{\tau(k)})$. A subset X in D^k is defined to be *symmetric* if for any $x \in X$ and any $\tau \in S_k$, $\tau \circ x \in X$. In particular, if X is symmetric and f is a symmetric function under the action of S_k , we then get the following useful counting formula for (2.2).

Proposition 2.2. *Let C_k be the set of conjugacy classes of S_k . If X is symmetric and f is symmetric, then*

$$F = \sum_{\tau \in C_k} \text{sign}(\tau) C(\tau) F_\tau, \quad (2.3)$$

where $C(\tau)$ is the number of permutations conjugate to τ .

For the purpose of our proof, we will also present several combinatorial formulas. A permutation $\tau \in S_k$ is said to be of type (c_1, c_2, \dots, c_k) if τ has exactly c_i cycles of length i . Denote by $N(c_1, c_2, \dots, c_k)$ to be the number of k -permutations of type (c_1, c_2, \dots, c_k) . It is well known that

$$N(c_1, c_2, \dots, c_k) = \frac{k!}{1^{c_1} c_1! 2^{c_2} c_2! \dots k^{c_k} c_k!}.$$

Lemma 2.3. *If we define the generating function*

$$C_k(t_1, t_2, \dots, t_k) = \sum_{\sum i c_i = k} N(c_1, c_2, \dots, c_k) t_1^{c_1} t_2^{c_2} \dots t_k^{c_k},$$

and set $t_1 = t_2 = \dots = t_k = q$, then

$$\begin{aligned} C_k(q, q, \dots, q) &= \sum_{\sum i c_i = k} N(c_1, c_2, \dots, c_k) q^{c_1} q^{c_2} \dots q^{c_k} \\ &= (q + k - 1)_k \end{aligned}$$

If we set $t_i = q$ for $d \mid i$ and $t_i = s$ for $d \nmid i$, then

$$\begin{aligned}
& C_k(\overbrace{s, \dots, s}^{d-1}, q, \overbrace{s, \dots, s}^{d-1}, q, \dots) \\
&= \sum_{\sum i c_i = k} N(c_1, c_2, \dots, c_k) q^{c_1} q^{c_2} \dots s^{c_d} q^{c_{d+1}} \dots \\
&= k! \sum_{i=0}^{\lfloor k/d \rfloor} \binom{\frac{q-s}{d} + i - 1}{\frac{q-s}{d} - 1} \binom{s+k-di-1}{s-1} \\
&\leq k! \binom{s+k+(q-s)/d-1}{k}.
\end{aligned}$$

3. SUBSET SUM PROBLEM IN A SUBSET OF THE RATIONAL POINT GROUP

Lemma 3.1 (Hasse-Weil Bound). *Let E be an elliptic curve over the finite field \mathbb{F}_q . Then the number of rational points on E has the following estimate*

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Lemma 3.2 (Structure of Rational Point Group). *A group G of order $N = q+1-m$ is isomorphic to $E(\mathbb{F}_q)$ for some elliptic curve E over \mathbb{F}_q if and only if one of the following conditions holds:*

- (i) $(q, m) = 1$, $|m| \leq 2\sqrt{q}$ and $G \cong \mathbb{Z}/A \times \mathbb{Z}/B$ where $B \mid (A, m-2)$.
- (ii) q is a square, $m = \pm 2\sqrt{q}$ and $G = (\mathbb{Z}/A)^2$ where $A = \sqrt{q} \mp 1$.
- (iii) q is a square, $p \equiv 1 \pmod{3}$, $m = \pm\sqrt{q}$ and G is cyclic.
- (iv) q is not a square, $p = 2$ or 3 , $m = \pm\sqrt{pq}$ and G is cyclic.
- (v) q is not a square, $p \equiv 3 \pmod{4}$, $m = 0$ and G is cyclic or q is a square, $p \equiv 1 \pmod{4}$, $m = 0$ and G is cyclic.
- (vi) q is not a square, $p \equiv 3 \pmod{4}$, $m = 0$ and G is either cyclic or $G \cong \mathbb{Z}/M \times \mathbb{Z}/2$ where $M = \frac{q+1}{2}$.

According to Lemma 3.2 on the structure of $E(\mathbb{F}_q)$, we may suppose that $G = E(\mathbb{F}_q) \cong \mathbb{Z}/n_1 \times \mathbb{Z}/n_2$ is a finite abelian group. By Lemma 3.1, G has order $q+1+c\sqrt{q}$, with $|c| \leq 2$. Denote by $\exp(G)$ the exponent of G . Let $D \subseteq G$ be a nonempty subset of cardinality n . Let \widehat{G} be the group of additive characters of G . Note that \widehat{G} is isomorphic to G . Define $s_\chi(D) = \sum_{a \in D} \chi(a)$ and $\Phi(D) = \max_{\chi \in \widehat{G}, \chi \neq \chi_0} |s_\chi(D)|$. Let $N(k, b, D)$ be the number of k -subsets $T \subseteq D$ such that $\sum_{x \in S} x = b$. In the following theorem we will give an asymptotic bound for $N(k, b, D)$ which ensures $N(k, b, D) > 0$ when $G - D$ is not too large compared with G .

Theorem 3.3. *Let $N(k, b, D)$ be defined as above.*

$$\begin{aligned}
\left| N(k, b, D) - |G|^{-1} \binom{n}{k} \right| &\leq \frac{|S|}{|G|} \binom{\Phi(D) + k - 1}{k} + \frac{1}{|G|} \binom{\frac{n+\Phi(D)}{2}}{k} \\
&\quad + \frac{1}{|G|} \sum_{\substack{2 \leq d \leq k \\ d \mid \exp(G)}} \phi(d) \binom{\frac{n+\Phi(D)}{d} + k - 1}{k}, \quad (3.1)
\end{aligned}$$

where S is the set of characters which has order greater than k .

Proof. Let $X = D \times D \times \dots \times D$ be the Cartesian product of k copies of D . Let $\overline{X} = \{(x_1, x_2, \dots, x_k) \in D^k \mid x_i \neq x_j, \forall i \neq j\}$. It is clear that $|X| = n^k$ and $|\overline{X}| = (n)_k$. We have

$$\begin{aligned}
k!N(k, b, D) &= |G|^{-1} \sum_{(x_1, x_2, \dots, x_k) \in \overline{X}} \sum_{\chi \in \widehat{G}} \chi(x_1 + x_2 + \dots + x_k - b) \\
&= |G|^{-1}(n)_k + |G|^{-1} \sum_{\chi \neq \chi_0} \sum_{(x_1, x_2, \dots, x_k) \in \overline{X}} \chi(x_1)\chi(x_2) \cdots \chi(x_k)\chi^{-1}(b) \\
&= |G|^{-1}(n)_k + |G|^{-1} \sum_{\chi \neq \chi_0} \chi^{-1}(b) \sum_{(x_1, x_2, \dots, x_k) \in \overline{X}} \prod_{i=1}^k \chi(x_i).
\end{aligned}$$

Denote $f_\chi(x) = f_\chi(x_1, x_2, \dots, x_k) = \prod_{i=1}^k \chi(x_i)$. For $\tau \in S_k$, let

$$F_\tau(\chi) = \sum_{x \in X_\tau} f_\chi(x) = \sum_{x \in X_\tau} \prod_{i=1}^k \chi(x_i),$$

where X_τ is defined as in (2.1). Obviously X is symmetric and $f_\chi(x_1, x_2, \dots, x_k)$ is normal on X . Applying (2.3) in Corollary 2.2, we get

$$k!N(k, b, D) = |G|^{-1}(n)_k + |G|^{-1} \sum_{\chi \neq \chi_0} \chi^{-1}(b) \sum_{\tau \in C_k} \text{sign}(\tau) C(\tau) F_\tau(\chi),$$

where C_k is the set of conjugacy classes of S_k , $C(\tau)$ is the number of permutations conjugate to τ . If τ is of type (c_1, c_2, \dots, c_k) , then

$$\begin{aligned}
F_\tau(\chi) &= \sum_{x \in X_\tau} \prod_{i=1}^k \chi(x_i) \\
&= \sum_{x \in X_\tau} \prod_{i=1}^{c_1} \chi(x_i) \prod_{i=1}^{c_2} \chi^2(x_{c_1+2i}) \cdots \prod_{i=1}^{c_k} \chi^k(x_{c_1+c_2+\dots+k i}) \\
&= \prod_{i=1}^k \left(\sum_{a \in D} \chi^i(a) \right)^{c_i} \\
&= n^{\sum c_i m_i(\chi)} s_\chi(D)^{\sum c_i (1-m_i(\chi))},
\end{aligned}$$

where $m_i(\chi) = 1$ if $\chi^i = 1$ and otherwise $m_i(\chi) = 0$.

Now suppose $\text{ord}(\chi) = d$ with $d \mid n_1 n_2$. Note that $C(\tau) = N(c_1, c_2, \dots, c_k)$. In the case $d = 2$, $s_\chi(D)$ is an integer. Applying Lemma 2.3, we have

$$\begin{aligned}
&\sum_{\tau \in C_k} \text{sign}(\tau) C(\tau) F_\tau(\chi) \\
&= (-1)^k \sum_{\tau \in C_k} C(\tau) (-n)^{\sum c_i m_i(\chi)} (-s_\chi(D))^{\sum c_i (1-m_i(\chi))} \\
&= (-1)^k k! \sum_{i=0}^{\lfloor k/2 \rfloor} \binom{\frac{-n+s_\chi(D)}{2} + i - 1}{i} \binom{-s_\chi(D) + k - 2i - 1}{k - 2i} \\
&= k! \sum_{i=0}^{\lfloor k/2 \rfloor} \binom{\frac{n-s_\chi(D)}{2}}{i} \binom{s_\chi(D)}{k - 2i} \\
&\leq k! \binom{\frac{n+\Phi(D)}{2}}{k}.
\end{aligned}$$

The last inequality in the case $s_\chi(D) > 0$ is from the identity

$$\sum_{i=0}^k \binom{a}{i} \binom{b}{k-i} = \binom{a+b}{k}.$$

In the case $s_\chi(D) < 0$, since the summation has alternative signs, the inequality follows from a simple combinatorial argument.

In the case $3 \leq d \leq k$, since $|s_\chi(D)| \leq \Phi(D)$, we have

$$\begin{aligned} & \sum_{\tau \in C_k} \text{sign}(\tau) C(\tau) F_\tau(\chi) \\ & \leq \sum_{\tau \in C_k} C(\tau) n^{\sum c_i m_i(\chi)} \Phi(D)^{\sum c_i (1-m_i(\chi))} \\ & \leq k! \binom{\frac{n+\Phi(D)}{d} + k - 1}{k}. \end{aligned}$$

Similarly, if $\text{ord}(\chi)$ is greater than k , then

$$\sum_{\tau \in C_k} \text{sign}(\tau) C(\tau) F_\tau(\chi) \leq k! \binom{\Phi(D) + k - 1}{k}.$$

Let S be the set of characters which have order greater than k . Summing over all nontrivial characters, we obtain

$$\begin{aligned} \left| N(k, b, D) - |G|^{-1} \binom{n}{k} \right| & \leq \frac{|S|}{|G|} \binom{\Phi(D) + k - 1}{k} + \frac{1}{|G|} \binom{\frac{n+\Phi(D)}{2}}{k} \\ & \quad + \frac{1}{|G|} \sum_{\substack{2 < d \leq k \\ d | \exp(G)}} \phi(d) \binom{\frac{n+\Phi(D)}{d} + k - 1}{k}, \end{aligned}$$

where $\phi(d)$ is the number of characters in \hat{G} of order d . This completes the proof. \square

Corollary 3.4. *We have*

$$\left| N(k, b, D) - |G|^{-1} \binom{n}{k} \right| \leq \binom{M}{k},$$

where M is defined as

$$M = \max \left\{ \binom{\Phi(D) + k - 1}{k}, \binom{\frac{n+\Phi(D)}{2}}{k}, \binom{\frac{n+\Phi(D)}{d} + k - 1}{k} \right\},$$

and d is the smallest nontrivial divisor of $|G|$ that is not equal to 2.

Corollary 3.5. *Let $q \geq 64$ and $n = q+2$. For $6 \leq k < q-1$, we have $N(k, b, D) > 0$ for every $b \in G$.*

Proof. By symmetry it is sufficient to consider the case $3 \leq k \leq n/2$. To ensure $N(k, b, D) > 0$, by (3.1) it suffices to have

$$\binom{n}{k} > |S| \binom{\Phi(D) + k - 1}{k} + \binom{\frac{n+\Phi(D)}{2}}{k} + \sum_{\substack{2 < d \leq k \\ d | \exp(G)}} \phi(d) \binom{\frac{n+\Phi(D)}{d} + k - 1}{k}.$$

For a nontrivial character χ , $\sum_{g \in G} \chi(g) = 0$ and it follows that $\Phi(D) = \Phi(G-D) < |G| - |D| \leq 2\sqrt{q} + 1$.

Since G is the product of at most two cyclic groups, by the definition of $\phi(d)$ we have $\phi(d) \leq d^2 - 1$. For simplicity, set $K = k^3 - 2k^2 - k + 2$. For the case $k \leq q^{1/3}$, it is sufficient to have

$$\binom{q+2}{k} - (q+2\sqrt{q}-K)\binom{2\sqrt{q}+k-1}{k} - \binom{\frac{q+2+2\sqrt{q}}{2}}{k} - K\binom{\frac{q+2\sqrt{q}}{3}+k-1}{k} > 0.$$

When $k = 3$, one has

$$125/216q^3 - 379/36q^{5/2} - 589/18q^2 + 593/27q^{3/2} + 149/2q + 67/3q^{1/2} > 0$$

It then suffices to have $q > 432$.

Similarly, when $k = 6$, one has $q \geq 64$. This is done by first taking $K = k^3 - 2k^2 - k + 2 = 140$, we solve that $q \geq 97$. But notice that now K should be ≤ 117 . Then taking $K = 117$, we solve $q \geq 79$. Iteratively, we can get $q \geq 64$ finally.

One checks that when $k \leq q^{1/3}$ this function is unimodal on k . For $q^{1/3} < k < (q+2\sqrt{q})/6$, it then suffices to have

$$\binom{q+2}{k} > (q+2+2\sqrt{q})\binom{\frac{q+2+2\sqrt{q}}{2}}{k},$$

and for $(q+2\sqrt{q})/6 \leq k \leq (q+2)/2$,

$$\binom{q+2}{k} > (q+2+2\sqrt{q})\binom{\frac{q+2\sqrt{q}}{3}+k-1}{k}.$$

It follows from a simple asymptotic analysis and the proof is complete. \square

A similar argument gives

Corollary 3.6. *Suppose that $n \geq (\frac{2}{3} + \epsilon)q$ and $q > \frac{4}{\epsilon^2}$, where ϵ is positive. Then there is a positive constant C_ϵ such that $N(k, b, D) > 0$ for every $b \in G$ provided $C_\epsilon \ln q < k < n - C_\epsilon \ln q$.*

Proof. Similar to the proof of the corollary above, we consider the case $k \leq n/2$. To ensure $N(k, b, D) > 0$, by (3.1) it suffices to have

$$\binom{n}{k} > |S|\binom{\Phi(D)+k-1}{k} + \binom{\frac{n+\Phi(D)}{2}}{k} + \sum_{\substack{2 < d \leq k \\ d | \exp(G)}} \phi(d)\binom{\frac{n+\Phi(D)}{d}+k-1}{k}.$$

For a nontrivial character χ , $\sum_{g \in G} \chi(g) = 0$ and it follows that $\Phi(D) = \Phi(G-D) < |G| - |D| \leq (\frac{1}{3} - \epsilon)q + 2\sqrt{q} + 1$.

For small $k \leq q/6$ it suffices to have

$$\binom{\frac{2q}{3}}{k} - (q+2\sqrt{q})\binom{\frac{q+2+2\sqrt{q}}{2}}{k} > 0,$$

i.e.,

$$\frac{(2/3q)_k}{((q+2+2\sqrt{q})/2)_k} \geq q+2\sqrt{q},$$

and then

$$\left(\frac{2/3q}{(q+2+2\sqrt{q})/2}\right)^k \geq q+2\sqrt{q},$$

which holds when

$$k > C \ln q$$

for some constant C .

For $q/6 < k \leq n/2 = (\frac{1}{3} + \frac{\epsilon}{2})q$, it suffices to have

$$\binom{(\frac{2}{3} + \epsilon)q}{k} > (q + 2\sqrt{q}) \binom{(\frac{2}{3} + \frac{\epsilon}{2})q + \sqrt{q}}{k},$$

which holds when $q > \frac{4}{\epsilon^2}$ and

$$k > C_\epsilon \ln q$$

for some constant C_ϵ . So, the proof is complete. \square

From the proof of the above corollary, it follows that

Corollary 3.7. *Suppose $n \geq (\frac{2}{3} + \epsilon)q$, where ϵ is positive and $\epsilon \leq 1/3$. When q is large enough (in application we need to use long length codes, so it is reasonable to assume q is large), then there is a positive constant C (independent of ϵ and q) such that $N(k, b, D) > 0$ for every $b \in G$ provided $C \ln q < k < n - C \ln q$.*

4. MINIMUM DISTANCE OF ELLIPTIC CODES AND SSP

In this section, we discuss the relationship between the minimum distance of ECAG code and SSP on the group of rational points of the elliptic curve. Using the results in the previous section, our main theorems in Introduction follow automatically.

We fix some notations for this section:

- X/\mathbb{F}_q is a geometrically irreducible smooth projective curve of genus g over the finite field \mathbb{F}_q with function field $\mathbb{F}_q(X)$.
- $X(\mathbb{F}_q)$ is the set of all \mathbb{F}_q -rational points on X .
- $D = \{P_1, P_2, \dots, P_n\}$ is a proper subset of rational points $X(\mathbb{F}_q)$.
- Without any confusion, we also write $D = P_1 + P_2 + \dots + P_n$.
- G is a divisor of degree k ($2g - 2 < k < n$) with $\text{Supp}(G) \cap D = \emptyset$.

Let V be a divisor on X . Denote by $\mathcal{L}(V)$ the \mathbb{F}_q -vector space of all rational functions $f \in \mathbb{F}_q(X)$ with the principal divisor $\text{div}(f) \geq -V$, together with the zero function (cf. [13]). It is well-known that $\mathcal{L}(V)$ is finite dimensional vector space over \mathbb{F}_q and $\dim \mathcal{L}(V) = k - g + 1$.

The functional AG code $C_{\mathcal{L}}(D, G)$ is defined to be the image of the following evaluation map:

$$\text{ev} : \mathcal{L}(G) \rightarrow \mathbb{F}_q^n; f \mapsto (f(P_1), f(P_2), \dots, f(P_n)).$$

As functions in $\mathcal{L}(G)$ have at most $\deg G$ zeros, the minimum distance of $C_{\mathcal{L}}(D, G)$ is $d \geq n - k$. Together with Riemann-Roch theorem, it is easy to see that the functional AG code $C_{\mathcal{L}}(D, G)$ has parameters $[n, k - g + 1, d \geq n - k]$. By the Singleton bound, we have

$$n - k \leq d \leq n - k + g.$$

If $X = E$ is an elliptic curve over \mathbb{F}_q , we only have the following two choices for the minimum distance of $C_{\mathcal{L}}(D, G)$:

$$d = n - k, \text{ or } d = n - k + 1.$$

Let \mathcal{G} be an abelian group with zero element O and D a finite subset of \mathcal{G} . For an integer $0 < k < |D|$ and an element $b \in D$, we denote

$$N_{\mathcal{G}}(k, b, D) = \#\{S \subseteq D \mid \#S = k \text{ and } \sum_{x \in S} x = b\}.$$

Computing $N_{\mathcal{G}}(k, b, D)$ is called the counting version of the k -subset sum problem (k -SSP). In general, the counting k -SSP is **NP**-hard. If there is no confusion, we simply denote

$$N(k, b, D) = N_{\mathcal{G}}(k, b, D).$$

Let E be an elliptic curve defined over \mathbb{F}_q with a rational point O . The set of rational points $E(\mathbb{F}_q)$ forms an abelian group with zero element O (for the definition for the sum of any two points, we refer to [12]), and it is isomorphic to the Picard group $\text{div}^o(E)/\text{Prin}(\mathbb{F}_q(E))$ where $\text{Prin}(\mathbb{F}_q(E))$ is the subgroup consisting of all principal divisors. Denote by \oplus and \ominus the additive and minus operator in the group $E(\mathbb{F}_q)$, respectively.

Proposition 4.1 ([3, 16]). *Let E be an elliptic curve over \mathbb{F}_q , $D = \{P_1, P_2, \dots, P_n\}$ a subset of $E(\mathbb{F}_q)$ such that rational points (not necessarily distinct) $O, P \notin D$ and let $G = (k-1)O + P$ ($0 < k < n$). Endow $E(\mathbb{F}_q)$ a group structure with the zero element O . Then the AG code $C_{\mathcal{L}}(D, G)$ is MDS, i.e., $d = n - k + 1$ if and only if*

$$N(k, P, D) = 0.$$

And the minimum distance $d = n - k$ if and only if

$$N(k, P, D) > 0.$$

Proof. We have already seen that the minimum distance of $C_{\mathcal{L}}(D, G)$ has two choices: $n - k$, $n - k + 1$. So $C_{\mathcal{L}}(D, G)$ is not MDS, i.e., $d = n - k$ if and only if there is a function $f \in \mathcal{L}(G)$ such that the evaluation $ev(f)$ has weight $n - k$. This is equivalent to that f has k zeros in D , say P_{i_1}, \dots, P_{i_k} . That is

$$\text{div}(f) \geq -(k-1)O - P + (P_{i_1} + \dots + P_{i_k}),$$

which is equivalent to

$$\text{div}(f) = -(k-1)O - P + (P_{i_1} + \dots + P_{i_k}).$$

The existence of such an f is equivalent to saying

$$P_{i_1} \oplus \dots \oplus P_{i_k} = P.$$

Namely, $N(k, P, D) > 0$. It follows that the AG code $C_{\mathcal{L}}(D, G)$ is MDS if and only if $N(k, P, D) = 0$. \square

Remark 4.2. In general, if G is a divisor of degree k on E , then for any rational point $Q \in E(\mathbb{F}_q)$, as $\deg(G - (k-1)Q) = 1$, by Riemann-Roch theorem, there exists one and only one rational point $P \in E(\mathbb{F}_q)$ such that $G \sim (k-1)Q + P$. Suppose there exist rational points Q, P such that $G \sim (k-1)Q + P$ and $P, Q \notin D$. Let $G' = (k-1)Q + P$. Then the codes $C_{\mathcal{L}}(D, G)$ and $C_{\mathcal{L}}(D, G')$ are equivalent [13, Proposition 2.2.14]. Here two codes $C_1, C_2 \subseteq \mathbb{F}_q^n$ are said to be *equivalent* if there is a vector $a = (a_1, \dots, a_n) \in (\mathbb{F}_q^*)^n$ such that

$$C_2 = a \cdot C_1 = \{(a_1 c_1, \dots, a_n c_n) \mid (c_1, \dots, c_n) \in C_1\}.$$

It is easy to see that two equivalent codes have the same weight distribution and hence the same minimum distance. So it suffices to consider all AG codes of the form $C_{\mathcal{L}}(D, (k-1)Q + P)$.

Proposition 4.1 establishes the relation between minimum distance of ECAG code and SSP on the rational point group of the elliptic curve. Together with Corollaries 3.5 and 3.6, we obtain the main results of this paper, Theorems 1.3-1.5.

Acknowledgements. This paper was written when the first author was visiting the Department of Mathematics at the University of Delaware and the Department of Mathematics at the University of California, Irvine. The first author would like to thank both departments for their hospitality.

REFERENCES

- [1] H. Chen. On the main conjecture of geometric MDS codes. *International Mathematics Research Notices*, 1994(8):313–318, 1994.
- [2] H. Chen and S.S.-T. Yau. Contribution to munuera’s problem on the main conjecture of geometric hyperelliptic MDS codes. *Information Theory, IEEE Transactions on*, 43(4):1349–1354, jul 1997.
- [3] Q. Cheng. Hard problems of algebraic geometry codes. *IEEE Transactions on Information Theory*, 54:402–406, 2008.
- [4] Q. Cheng and D. Wan. A deterministic reduction for the gap minimum distance problem:[extended abstract]. In *Proceedings of the 41st annual ACM symposium on Theory of computing*, pages 33–38. ACM, 2009.
- [5] M.A. de Boer. MDS codes from hyperelliptic curves. *Arithmetic, Geometry and Coding Theory*, pages 23–34, 1996.
- [6] I. Dumer, D. Micciancio, and M. Sudan. Hardness of approximating the minimum distance of a linear code. *Information Theory, IEEE Transactions on*, 49(1):22–37, 2003.
- [7] G.L. Katsman and M.A. Tsfasman. Spectra of algebraic-geometric codes. *Problemy Peredachi Informatsii*, 23(4):19–34, 1987.
- [8] J.Y. Li and D. Wan. A new sieve for distinct coordinate counting. *Science China-mathematics*, 53:1–12, 2010.
- [9] J.Y. Li and D. Wan. Counting subset sums of finite abelian groups. *Journal of Combinatorial Theory, Series A*, 119(1):170 – 182, 2012.
- [10] F. MacWilliams and N. Sloane. The theory of error-correcting codes. *North-Holland*, 2006.
- [11] C. Munuera. On the main conjecture on geometric MDS codes. *Information Theory, IEEE Transactions on*, 38(5):1573–1577, 1992.
- [12] J.H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.
- [13] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.
- [14] A. Vardy. The intractability of computing the minimum distance of a code. *Information Theory, IEEE Transactions on*, 43(6):1757–1766, 1997.
- [15] J.L. Walker. A new approach to the main conjecture on algebraic-geometric MDS codes. *Designs, Codes and Cryptography*, 9(1):115–120, 1996.
- [16] J. Zhang, F.W. Fu, and D. Wan. Stopping set distributions of algebraic geometry codes from elliptic curves. In *Proceedings of the 9th Annual international conference on Theory and Applications of Models of Computation*, TAMC’12, pages 295–306, Berlin, Heidelberg, 2012. Springer-Verlag.

DEPARTMENT OF MATHEMATICS, SHANGHAI JIAO TONG UNIVERSITY, SHANGHAI, P.R. CHINA
AND DEPARTMENT OF MATHEMATICS, UNIVERSITY OF DELAWARE, USA

E-mail address: `lijiyou@sjtu.edu.cn`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, IRVINE, CA 92697-3875, USA

E-mail address: `dwan@math.uci.edu`

SCHOOL OF MATHEMATICS, CAPITAL NORMAL UNIVERSITY

E-mail address: `junz@cnu.edu.cn`